Attorney Docket No. 1405.1049

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Toru KAMIWADA, et al.

Application No.: Group Art Unit:

Filed: September 19, 2001 Examiner:

For: DEVICE CONTROL SYSTEM

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. §1.55

Assistant Commissioner for Patents
Washington, D.C. 2023l

Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No. 2001-160083

Filed: May 29, 2001

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. §119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: September 19, 2001 By: _____

James D. Halsey, Jr.
Registration No. 22,729

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年 ５月２９日

出願番号
Application Number: 特願２００１－１６００８３

出願人
Applicant(s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ８月１０日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願

【整理番号】　0195025

【提出日】　平成13年 5月29日

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 17/60

【発明の名称】　機器制御システム

【請求項の数】　5

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　上和田　徹

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　浅見　俊宏

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　藤田　卓志

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100094145

【弁理士】

【氏名又は名称】　小野　由己男

【連絡先】　０６－６３１６－５５３３

【選任した代理人】

【識別番号】　100094167

【弁理士】

【氏名又は名称】　宮川　良夫

【選任した代理人】

【識別番号】　100106367

【弁理士】

【氏名又は名称】　稲積　朋子

【手数料の表示】

【予納台帳番号】　020905

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9807456

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　機器制御システム

【特許請求の範囲】

【請求項１】

有線または無線の宅内ネットワークを介して住宅内の１以上の機器に接続される機器制御サーバと、前記機器の操作に関する指示信号を有線または無線で送信可能な操作端末とを備える機器制御システムのアクセス制限方法であって、

前記操作端末に設定される固有の識別子を前記操作端末のアクセス権と関連付けるための端末情報の登録を受け付ける段階と、

前記操作端末の識別子と前記機器の操作に関する指示信号とを含む指示情報を受け付ける段階と、

前記指示情報に含まれる前記操作端末の識別子から前記操作端末のアクセス権を判定する段階と、

前記操作端末のアクセス権と前記機器に関する指示信号とに基づいて前記機器の制御を行う段階と、

を含む機器制御システムのアクセス制御方法。

【請求項２】

請求項１に記載の機器制御システムのアクセス制御方法をコンピュータに実行させるためのプログラム。

【請求項３】

請求項２に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項４】

有線または無線の宅内ネットワークを介して住宅内の１以上の機器に接続され、操作端末から送信される前記機器の操作に関する指示信号に基づいて前記機器の制御を行う機器制御サーバであって、

前記操作端末に設定される固有の識別子を前記操作端末のアクセス権と関連付けるための端末情報の登録を受け付ける端末情報受付手段と、

前記操作端末の識別子と前記機器の操作に関する指示信号とを含む指示情報を

受け付ける指示情報受付手段と、

前記指示情報に基づいて前記操作端末のアクセス権を判定するアクセス権判別手段と、

前記アクセス権判別手段により判定された前記操作端末のアクセス権と前記指示情報に含まれる前記機器の操作に関する指示信号とに基づいて前記機器の制御を行う機器制御手段と、

を含む機器制御サーバ。

【請求項５】

住宅内の１以上の機器と有線または無線の宅内ネットワークを介して接続される機器制御サーバを有する機器制御システムにおける前記機器の操作に関する指示信号を送信する操作端末であって、

固有の識別子を記憶する識別子記憶手段と、

前記機器制御サーバに前記識別子の登録を行う端末情報登録手段と、

前記の操作に関する指示入力を受け付ける入力受付手段と、

前記入力受付手段により受け付けた指示入力と、前記識別子記憶手段に記憶されている識別子とに基づいて指示情報を生成する指示情報生成手段と、

前記指示情報生成手段により生成された指示情報を無線または有線により送信する指示情報送信手段と、

を備える操作端末。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、家庭内のテレビやビデオなどのＡＶ機器、電話やパソコンなどの情報通信機器、エアコンや冷蔵庫などの家電機器について、家庭内および宅外からリモコンなどの操作端末を用いて動作制御を行ったり、ホームサーバ内に蓄積されている情報や、ホームサーバ経由で外部から取得できる情報を無線または有線の情報通信技術を介して利用するための機器制御システムに関する。

【０００２】

【従来の技術】

家庭内の機器を遠隔操作するためのリモコンは、多くの場合には各機器と１対１で対応しており、このため複数の機器の操作を行うためには複数のリモコンが必要となる。これに対し、複数のリモコンが発信する信号を記憶させ、１つの操作端末で複数の機器を操作できるようにした統合型リモコンが提案されている。この統合型リモコンを用いた場合には、住宅内において各機器を制御することは可能であるが、宅外から各機器の制御を行うことが不可能である。

【０００３】

家庭内のテレビやビデオなどのＡＶ機器、電話やパソコンなどの情報通信機器、エアコンや冷蔵庫などの家電機器を宅内ネットワークで接続し、この宅内ネットワークに接続された機器制御サーバ（ホームサーバ）により各機器の制御を行うようにした機器制御システムの構成が考えられる。この場合、宅外からのアクセスには、ネットワークを介してホームサーバに接続することとなり、第３者からの不正なアクセスを防止するために、操作者の認証を行う必要性がでてくる。たとえば、各機器の操作を行うためのパスワードを設定しておき、機器の操作に関する指示を行う場合に操作端末からのパスワードの入力を受け付け、認証を行うことで第３者による不正なアクセスを防止することが可能となる。

【０００４】

また、ホームサーバでは取得した各種情報を蓄積するための蓄積手段や宅外ネットワークを介して外部から取得可能な各種情報の提供を行うための外部接続手段などを備えている場合がある。このような各種情報を提供するためには、認証を行って利用者の特定を行う必要がある場合がでてくる。たとえば、未成年に見せることが好ましくないような映像コンテンツでは、その映像コンテンツを取り出してテレビに出力する前に、出力してもよいか否かの判定を行う必要となる。この場合も、利用者を特定するための認証情報としてパスワードの入力を要求し、利用者から入力されたパスワードが正当なものであるか否かを判断することにより、テレビなどの機器を制御してそのコンテンツの出力に関する制御を行うことが考えられる。

【０００５】

各機器が設置されている住宅内からのアクセスである場合と宅外からのアクセ

スである場合を区別するために、各操作端末に異なるパスワードを設定することが考えられる。また、利用するコンテンツ毎やコンテンツの種別毎にパスワードを設定しておくことも可能である。このようにすることで１つのパスワードが第３者に知られてしまった場合であっても、その第３者によるアクセスが他の部分に影響することを抑制でき、不正なアクセスによる影響を最小限にとどめることができる。

【０００６】

【発明が解決しようとする課題】

前述したような機器制御システムにおいて、住宅内または宅外からホームサーバにアクセスを行う際にユーザの認証が必要となる場合、その都度パスワードの入力が必要となり作業が煩雑となる。また、このようなパスワード入力のみによる認証では、第３者にパスワードを知られてしまうとその者による不正なアクセスが可能となってしまう。

【０００７】

パスワードを定期的に変更することにより、不正なアクセスを抑制する効果があるが、完全に不正なアクセスを防止できるものではなく、パスワードを変更する手間がかかり、利用者にとって煩雑な作業が必要となるとともに、パスワードを忘れるという確率が高くなる。アクセス元となる操作端末毎に異なるパスワードを設定した場合やコンテンツやサービス毎にパスワードを設定した場合にも、利用者がそれぞれのパスワードを憶えておく必要があり、忘れてしまう確率も高くなる。

【０００８】

パスワードをリモコンやその他の操作端末に記憶させておき、パスワード入力の手間を省くことも考えられるが、このパスワードを第３者に知られてしまった場合に、不正なアクセスを防止することができない。特に、宅外からの不正なアクセスにより家庭内の情報が引き出されたり、改変された場合には、非常な不都合を生じるおそれがある。

【０００９】

本発明は、住宅内の機器を制御する機器制御システムにおいて、利用者の認証

作業の手間を軽減するとともに、第３者からの不正なアクセスを防止することを目的とする。

【００１０】

【課題を解決するための手段】

本発明に係る機器制御システムのアクセス制限方法は、有線または無線の宅内ネットワークを介して住宅内の１以上の機器に接続される機器制御サーバと、機器の操作に関する指示信号を有線または無線で送信可能な操作端末とを備える機器制御システムのアクセス制限方法であって、操作端末に設定される固有の識別子を操作端末のアクセス権と関連付けるための端末情報の登録を受け付ける段階と、操作端末の識別子と機器の操作に関する指示信号とを含む指示情報を受け付ける段階と、指示情報に含まれる操作端末の識別子から操作端末のアクセス権を判定する段階と、操作端末のアクセス権と機器に関する指示信号とに基づいて機器の制御を行う段階とを含む。

【００１１】

ここで、端末情報の登録を受け付ける際に操作端末に設定される公開鍵を受け付け、操作端末において秘密鍵で暗号化された所定のデータを受信し、公開鍵により復号化して所定のデータと照合することによって操作端末の認証を行う段階をさらに含む構成とすることができる。

【００１２】

また、電子情報を取得するとともに蓄積手段内に蓄積する段階をさらに含み、機器に関する指示信号が蓄積手段に蓄積された電子情報へのアクセスを含む場合に、操作端末のアクセス権に基づいて電子情報の提供を許可するか否かを判断するように構成できる。

【００１３】

さらに、機器の操作に関する指示信号が宅外ネットワークへのアクセスを含む場合に、操作端末のアクセス権に基づいて宅外ネットワークへのアクセスを許可するか否かを判断し機器の制御を行うように構成できる。この場合には、宅外ネットワーク上のコンテンツ毎にアクセスを許可するか否かを判断するように構成することも可能である。

【００１４】

また、操作端末からの指示情報を受信した際に、操作端末が宅内にあるか宅外にあるかを判別し、この判別結果と指示情報に含まれる操作端末の識別子から操作端末のアクセス権を判定するように構成できる。

【００１５】

さらに、操作端末を操作するユーザに関する情報を操作端末と関連付けるための個人情報の登録を受け付ける段階をさらに含み、指示情報に含まれる操作端末の識別子からこの操作端末に関連付けられた個人情報を抽出し、個人情報および端末情報からアクセス権を判定するように構成できる。

【００１６】

本発明では、上述したような機器制御システムのアクセス制御方法をコンピュータに実行させるためのプログラムを提案する。

また、本発明では、このような機器制御システムのアクセス制御方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体を提案する。

【００１７】

本発明に係る機器制御サーバは、有線または無線の宅内ネットワークを介して住宅内の１以上の機器に接続され、操作端末から送信される機器の操作に関する指示信号に基づいて機器の制御を行う機器制御サーバであって、操作端末に設定される固有の識別子を操作端末のアクセス権と関連付けるための端末情報の登録を受け付ける端末情報受付手段と、操作端末の識別子と機器の操作に関する指示信号とを含む指示情報を受け付ける指示情報受付手段と、指示情報に基づいて操作端末のアクセス権を判定するアクセス権判別手段と、アクセス権判別手段により判定された操作端末のアクセス権と指示情報に含まれる機器の操作に関する指示信号とに基づいて機器の制御を行う機器制御手段とを含む。

【００１８】

ここで、端末情報の登録を受け付ける際に、操作端末に設定される公開鍵を受け付け、端末情報とともに端末情報記憶手段に格納する公開鍵受付手段と、所定のデータを送信し、操作端末において秘密鍵で暗号化された所定のデータを受信

し、公開鍵により復号化して所定のデータと照合することによって、操作端末の認証を行う操作端末認証手段とをさらに含む構成とすることができる。

【００１９】

また、端末情報受付手段は、端末情報の一部として操作端末の識別子と関連付けられる公開鍵の登録を受け付けるように構成できる。

さらに、電子情報を取得する電子情報取得手段と、電子情報取得手段により取得した電子情報を蓄積する電子情報蓄積手段とをさらに備え、機器に関する指示信号が電子情報蓄積手段に蓄積された電子情報へのアクセスを含む場合に、アクセス権判定手段は、操作端末のアクセス権を判定して電子情報の提供を許可するか否かを判断するように構成できる。

【００２０】

また、住宅外に存在する宅外ネットワークに接続可能な宅外通信手段をさらに備え、機器の操作に関する指示信号が宅外ネットワークへのアクセスを含む場合に、アクセス権判定手段は、操作端末のアクセス権を判定し宅外ネットワークへのアクセスを許可するか否かを判断するように構成できる。この場合、宅外ネットワーク上のコンテンツ毎にアクセスを許可するか否かを判断するように構成することも可能である。

【００２１】

さらに、指示情報受付手段により受け付けた指示情報に基づいて、操作端末が宅内にあるか宅外にあるかを判別する端末位置判別手段をさらに備え、アクセス権判定手段は、端末位置判別手段による判別結果に基づいて操作端末のアクセス権を判定するように構成できる。

【００２２】

また、操作端末を操作するユーザに関する情報を操作端末と関連付けるための個人情報の登録を受け付ける個人情報受付手段をさらに含み、アクセス権判定手段は、指示情報に含まれる操作端末の識別子からこの操作端末に関連付けられた個人情報を抽出し、個人情報および前記端末情報からアクセス権を判定するように構成できる。

【００２３】

本発明に係る操作端末は、住宅内の１以上の機器と有線または無線の宅内ネットワークを介して接続される機器制御サーバを有する機器制御システムにおける機器の操作に関する指示信号を送信する操作端末であって、固有の識別子を記憶する識別子記憶手段と、識別子を機器制御サーバに登録する端末情報登録手段と、機器の操作に関する指示入力を受け付ける入力受付手段と、入力受付手段により受け付けた指示入力と識別子記憶手段に記憶されている識別子とに基づいて指示情報を生成する指示情報生成手段と、指示情報生成手段により生成された指示情報を無線または有線により送信する指示情報送信手段とを備える。

【００２４】

ここで、現在の位置情報を取得する位置情報取得手段をさらに備え、指示情報生成手段は、指示入力、識別子および位置情報取得手段により取得した位置情報に基づいて指示情報を生成するように構成できる。

【００２５】

また、操作するユーザに関する情報の入力を受け付ける個人情報入力手段をさらに備え、指示情報生成手段は、指示入力、識別子および個人情報入力手段により受け付けたユーザに関する情報に基づいて指示情報を生成するように構成できる。

【００２６】

さらに、指示情報を暗号化するための暗号鍵を格納する暗号鍵記憶手段をさらに備え、指示情報生成手段は、暗号鍵記憶手段に記憶されている暗号鍵により指示入力と識別子を暗号化して指示情報を生成するように構成できる。

【００２７】

また、秘密鍵を記憶する秘密鍵記憶手段と、秘密鍵に対応する公開鍵を記憶する公開鍵記憶手段と、秘密鍵によりデータを暗号化する暗号化処理手段とをさらに含み、端末情報登録手段により機器制御サーバに端末情報の登録を行う際に公開鍵を機器制御サーバに送信し、指示情報を送信する際に、機器制御サーバから受信する所定のデータを秘密鍵によって暗号化して認証情報として送信する構成とすることが可能である。

【００２８】

【発明の実施の形態】

〈概略構成〉

本発明の１実施形態が採用される機器制御システムの概略構成を図１に示す。

【００２９】

住宅内に設置されるテレビ５１やビデオ５２などのＡＶ機器、パソコン５３や電話機５４などの情報通信機器、エアコン５５や冷蔵庫５６などの家電機器などは、宅内ネットワーク５によってホームサーバ１に接続されている。宅内ネットワーク５は、有線または無線で構成することが可能であり、たとえば、Ｅｔｈｅｒｎｅｔや電灯線ＬＡＮなどの有線によるＬＡＮ、Ｂｌｕｅｔｏｏｔｈ、ＨｏｍｅＲＦ、ＩＥＥＥ８０２．１１Ｂなどの電波を用いた無線通信手段やＩｒＤＡなどの赤外線を用いた無線通信手段などによる無線によるＬＡＮなどを採用し得る。

【００３０】

テレビ５１、ビデオ５２、パソコン５３、電話機５４、エアコン５５、冷蔵庫５６などの機器は、リモコン３による操作が可能となっている。このリモコン３は、たとえば、機器の操作に関する指示入力を受け付けるための操作ボタン、受け付けた指示入力に基づいて指示情報を送信するとともに機器などからのデータを受信するための赤外線送受信手段、受け付けた操作内容や機器などから受信したデータを表示するための表示手段などを備えるものである。リモコン３は、各機器に指示情報を送信するように構成することも可能であり、また、ホームサーバ１に指示情報を送信するように構成することも可能である。

【００３１】

ホームサーバ１は、地上波受信用アンテナ、衛生放送受信用アンテナまたはＣＡＴＶのケーブル接続部などの放送受信手段８を介して、画像情報、音声情報および文字情報などを受信することが可能となっており、受信した情報をテレビ５１やビデオ５２を介してユーザに提供することが可能となっている。

【００３２】

また、ホームサーバ１は、電話回線網やインターネット網などの宅外ネットワーク７と接続されており、パソコン５３や電話機５４から外部とのデータの送受

信を行うことを可能とする。

【００３３】

ホームサーバ１は、たとえば図２に示すような構成となっている。

ホームサーバ１は、各種情報を受け付けるための操作パネル１１を備えている。この操作パネル１１は、有線または無線で接続されたキーボードや操作ボタンなどで構成することが可能であり、ホームサーバにＣＲＴや液晶表示パネルなどを備えている場合には、マウスやトラックボールなどのポインティングデバイスで構成することも可能である。操作パネル１１から入力された各種情報は、入力処理部１２によって受け付けられ、通信制御部１５により対応する部分に送信される。

【００３４】

また、ホームサーバ１は、宅内ネットワーク５と接続される宅内通信部１３を備えている。この宅内通信部１３は、宅内ネットワーク５とデータの送信を行うものであり、前述したようなＥｔｈｅｒｎｅｔや電灯線ＬＡＮなどの有線によるＬＡＮ、Ｂｌｕｅｔｏｏｔｈ、ＨｏｍｅＲＦ、ＩＥＥＥ８０２．１１Ｂなどの電波を用いた無線通信手段やＩｒＤＡなどの赤外線を用いた無線通信手段などによる無線によるＬＡＮに対応するインターフェイスで構成することができる。

【００３５】

さらにホームサーバ１は、宅外ネットワーク７と接続される宅外通信部１４を備えている。この宅外通信部１４は、電話通信網やインターネット網に接続するためのルータやモデムなどで構成することができる。

【００３６】

また、ホームサーバ１は、放送受信手段８によって受信される画像情報、音声情報、文字情報などの情報を受け付ける放送受信部２１を備えている。放送受信部２１は、受信した情報を蓄積情報データベース２３に蓄積するか否かを管理する蓄積情報管理部２２に接続されている。蓄積情報データベース２３は、ハードディスクドライブやＭＯ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤなどの記録メディアを用いたデータ格納手段で構成することが可能である。

【００３７】

入力処理部１２、宅内通信部１３、宅外通信部１４、蓄積情報管理部２２は通信制御部１５に接続されている。通信制御部１５は、さらにアクセス権制御部１６に接続されている。アクセス権制御部１６は、端末情報管理部１７と個人情報管理部１８に接続されている。

【００３８】

端末情報管理部１７は、リモコン３や操作パネル１１などから入力される端末情報に基づいて端末情報データベース１９を更新するとともに、アクセス権制御部１６からの要求に応じて端末情報データベース１９の内容を読み出して端末情報を提供するものである。

【００３９】

個人情報管理部１８は、リモコン３や操作パネル１１などから入力される個人情報に基づいて個人情報データベース２０を更新するとともに、アクセス権制御部１６からの要求に基づいて個人情報データベース２０の内容を読み出して個人情報を提供するものである。

【００４０】

通信制御部１５は、ユーザや各機器から送信されてくる指示情報に基づいて、各機器から送出される情報、宅外通信部１４で受信した情報、放送受信部２１で受信した情報、蓄積情報データ２３内の蓄積情報などを指示情報に対応する機器などに送信してユーザに提供し、リモコン３などの操作端末に関する端末情報や操作端末を使用するユーザの個人情報などの登録情報を受信した場合に、端末情報管理部１７および個人情報管理部１８に送信して各情報の登録を行わせるものである。

【００４１】

リモコン３の概略構成を図３に示す。

リモコン３は、ユーザからの指示入力を受け付けるための入力装置３９を備えている。入力装置３９は、通常の押しボタンスイッチなどで構成されるものであり、液晶表示パネル上に透明電極が重ねて配置されたタッチパネルで構成することも可能である。

【００４２】

リモコン３は、ユーザから受け付けた指示入力の内容や現在のリモコンの動作モード、各機器の動作モード、その他の情報を表示するための表示装置４０を備えている。表示装置４０は、液晶表示パネルやＬＥＤ、ＥＬなど表示デバイスを採用することが可能である。

【００４３】

また、リモコン３は、各機器またはホームサーバ１と通信可能な通信装置４１が設けられている。通信装置４１は、ＩｒＤＡなどの赤外線通信プロトコルを用いた通信手段が採用され、また、Ｂｌｕｅｔｏｏｔｈ、HomeＲＦ、ＩＥＥＥ８０２．１１Ｂなどの電波を用いた通信手段を用いることも可能で、さらに有線により機器またはホームサーバ１に接続された構成とすることも可能である。

【００４４】

リモコン３の内部には、各部を制御するための中央制御部３４を備えている。この中央制御部３４には、入力処理部３１、表示処理部３２、通信処理部３３、端末ＩＤ記憶部３５、公開鍵記憶部３６、暗号化処理部３７などが接続されている。

【００４５】

入力処理部３１は、入力装置３９から入力されるユーザの指示入力を受け付ける。表示処理部３２は、入力装置３９から入力された指示入力の内容やリモコン３の動作モードや各機器の動作モード、その他の情報を表示装置４０に送信してこれを表示させるものである。通信処理部３３は、ユーザから入力された指示入力に基づく指示情報を各機器またはホームサーバ１に送信するとともに、各機器の動作モードや動作状態に関する情報を受信して中央制御部３４に送信する。

【００４６】

端末ＩＤ記憶部３５は、リモコン３に設定される固有の識別子を記憶するものであり、予め設定された製品ＩＤや設定権を有する者が入力装置３９などから入力した固有ＩＤを格納する。この端末ＩＤ記憶部３５は、ＲＯＭ、ＥＥＰＲＯＭ、電源バックアップされたＲＡＭなどの記憶デバイスで構成することが可能である。

【００４７】

公開鍵記憶部３６は、操作端末毎に設定され指示情報の送信先であるホームサーバ１などに予め送信しておく公開鍵を格納しておくものである。この公開鍵記憶部３６は、ＲＯＭ、ＥＥＰＲＯＭ、電源バックアップされたＲＡＭなどの記憶デバイスで構成することが可能である。

【００４８】

暗号化処理部３７は、秘密鍵記憶部３８に格納されている暗号鍵に基づいて、送信する指示情報を暗号化するものであり、秘密鍵記憶部３８とともにＩＣチップ化された論理演算回路で構成することができる。

【００４９】

〈登録処理〉

リモコン３を各機器の操作端末として登録する場合の動作を説明する。

ホームサーバ１における登録処理のフローチャートを図４に示す。

【００５０】

ホームサーバ１は、ステップＳ１１において、宅内通信部１３を介して端末情報を受信し、この端末情報を通信制御部１５、アクセス権制御部１６、端末情報管理部１７を介して端末情報データベースに格納するための登録受付状態に設定する。ステップＳ１２では、登録受付状態の開始時刻t_0に現在時刻を代入する。

【００５１】

ステップＳ１３では、操作端末から登録要求があったか否かを判別する。リモコン３から登録要求を受信した場合にはステップＳ１７に移行し、リモコン３からの登録要求がない場合にはステップＳ１４に移行する。

【００５２】

ステップＳ１４では、登録中止ボタンが入力されたか否かを判別する。リモコン３から登録中止の指示入力を受け付けた場合にはステップＳ１６に移行し、登録中止の指示入力がない場合にはステップＳ１５に移行する

ステップＳ１５では、時刻t_0からの経過時間が所定時間t_{MAX}以上となったか否かを判別する。登録受付状態の開始から所定時間t_{MAX}が経過した判断した場合にはステップＳ１６に移行し、そうでない場合にはステップＳ１３に移行する

。

【００５３】

ステップＳ１６では、登録受付状態を解除して処理を終了する。

ステップＳ１７では、登録受付状態の解除を行う。ここでは、登録要求を送信してきたリモコン３に対して登録要求受理信号を送信し、他の操作端末からの新たな登録要求を禁止する。

【００５４】

ステップＳ１８では、操作端末から端末ＩＤと公開鍵を受信する。ここでは、リモコン３の端末ＩＤ記憶部３５に格納されているリモコン３の識別子と、公開鍵記憶部３６に格納されている公開鍵を受信する。この場合、リモコン３から送信される端末ＩＤと公開鍵の情報を、宅内ネットワーク５に接続された各機器のうちのいずれかで受信し、これをホームサーバ１の宅内通信部１４に送信させるように構成することもでき、また、ホームサーバ１により直接リモコン３からの情報を受信するように構成することもできる。

【００５５】

ステップＳ１９では、受信した操作端末の端末ＩＤおよび公開鍵を記録する。ここでは、リモコン３に設定された固有の識別子と公開鍵を端末情報データベース１９内に格納する。

【００５６】

登録処理時のリモコン３における動作を図５のフローチャートに示す。

ステップＳ２１では、登録要求を送信する。ここでは、通信装置４１を用いて宅内ネットワーク５に接続されている機器のうちのいずれかまたはホームサーバ１に直接登録要求信号を送信する。

【００５７】

ステップＳ２２では、登録要求が受理されたか否かを判別する。ホームサーバ１から送出される登録要求受理信号を受信した場合には、ステップＳ２３に移行する。

【００５８】

ステップＳ２３では、端末ＩＤと公開鍵の送信を行う。ここでは、端末ＩＤ記

憶部３５に格納されているリモコン３に固有の識別子および公開鍵記憶部３６に格納されている公開鍵を読み出して、通信装置４１を介して送信する。

【００５９】

〈操作端末の認証〉

操作端末を用いてホームサーバにアクセスする際の、操作端末の認証の手順を説明する。

【００６０】

操作端末からのアクセスを受け付ける際に、ホームサーバ１が行う操作端末の認証の動作を図６のフローチャートを用いて説明する。

ステップＳ３１では、操作端末の端末ＩＤを受け付ける。ここでは、リモコン３から送信される端末ＩＤを宅内通信部１３などを介して受信してこれを受け付ける。

【００６１】

ステップＳ３２では、登録されている端末情報から、送信されてきた端末ＩＤに対応する端末情報を取り出す。ここでは、端末情報データベース１９内を検索して、受信した端末ＩＤに対応する端末情報を抽出する。

【００６２】

ステップＳ３３では、受信した端末ＩＤが登録されている操作端末であるか否かを判別する。端末情報データベース１９に登録されていない端末ＩＤである場合には、認証失敗のエラーメッセージを操作端末に送信し処理を終了する。また、端末情報データベース１９に端末ＩＤが存在する場合にはステップＳ３４に移行する。

【００６３】

ステップＳ３４では、認証用データ列Ａを生成する。ここでは、認証用データとして所定の方法でデータ列Ａを生成する。ステップＳ３５では、認証用データ列Ａを操作端末に送信する。ステップＳ３６では、操作端末で暗号化されたデータ列Ｂを受信する。このデータ列Ｂは、送信した認証用データＡを操作端末側において秘密鍵によって暗号化したものである。ステップＳ３７では、受信したデータ列Ｂを操作端末に対応する公開鍵で復号化する。ここでは、端末情報データ

ベース１９から抽出した端末情報に含まれる公開鍵を用いて、データ列Ｂを復号化する。

【００６４】

ステップＳ３８では、復号化したデータがデータ列Ａと一致するか否かを判別する。リモコン３の秘密鍵記憶部３８に格納されている秘密鍵で暗号化されたデータは、対応する公開鍵でのみ復号できるように構成されており、秘密鍵で暗号化されたデータ列Ｂを送信してきた操作端末が正当な操作端末であれば、公開鍵で復号化されたデータが元の認証用データ列Ａと一致するはずである。復号化されたデータ列が認証用データ列Ａと一致した場合には認証成功した旨のメッセージを送信し、機器の操作に関する指示情報を受け付ける。また、復号化されたデータ列が認証用データ列Ａと一致しない場合には、認証失敗のエラーメッセージを操作端末に送信し処理を終了する。

【００６５】

リモコン３からアクセスを行う際の操作端末認証時の動作を図７のフローチャートを用いて説明する。

ステップＳ４１では、ホームサーバ１から送信されてくる認証用のデータ列Ａを受信する。ステップＳ４２では、受け取った認証用のデータ列Ａを秘密鍵で暗号化する。ここでは、秘密鍵記憶部３８に格納されている秘密鍵を用いて暗号化処理部３７がデータ列Ａを暗号化して暗号化データ列Ｂを生成する。秘密鍵記憶部３８に格納されている秘密鍵は、外部からの読み出しができないように構成されており、暗号化処理部３７による暗号化にのみ用いられるように構成されている。

【００６６】

ステップＳ４３では、暗号化したデータ列Ｂをホームサーバ１に送信する。ここでは、通信装置４１を用いて宅内ネットワーク５に接続されている機器のうちいずれか、またはホームサーバ１に直接送信する。

【００６７】

ステップＳ４４では、認証に成功したか否かを判別する。ホームサーバ１から認証に成功した旨のメッセージを受信した場合には次の処理に移行する。ホーム

サーバ１から認証に失敗した旨のメッセージを受信した場合には、認証失敗のメッセージを表示装置４０に表示して処理を終了する。

【００６８】

〈操作制御〉

実際にリモコン３から各機器の指示情報を送信して操作する場合の例を説明する。

【００６９】

ホームサーバ１では、放送受信部２１を介して受信した動画像データを蓄積情報データベース２３に格納することが可能となっている。この蓄積情報データベース２３に蓄積されている動画像データをリモコン３から操作してテレビ５１に表示させる場合について説明する。テレビ５１は、リモコン３によりチャンネル選択やメニュー選択などの操作を行うことが可能となっており、宅内ネットワーク５を介してホームサーバ１と接続されている。

【００７０】

リモコン３によりテレビのメニューを選択し、ホームサーバ１にある情報の一覧を表示するように要求する。このメニュー選択を受けて、テレビ５１はホームサーバ１と通信を行い、蓄積情報データベース２３内に蓄積されている情報の一覧情報を要求する。この一覧情報の要求時に、指示情報が送信されたリモコン３の端末ＩＤも併せて送信する。

【００７１】

一覧情報の要求を受けたホームサーバ１は、受け取った端末ＩＤを元に操作端末の認証処理を実行する。前述したように、認証用の文字列Ａを生成してこれを送信して、秘密鍵で暗号化された文字列Ｂを受信し、これを公開鍵で復号化して文字列Ａと照合することによって、操作端末の認証を行うことができる。操作端末の認証に成功した場合には、蓄積情報データベース２３内に蓄積されている情報の一覧を送信する。

【００７２】

テレビ５１では、ホームサーバ１から送信されてきた一覧情報を表示し、ユーザに見たい動画像データの選択を行わせる。この動画像データの選択についても

、リモコン３の操作により送信される指示情報をテレビ５１により受け付けて、宅内ネットワーク５を介してホームサーバ１に送信するように構成する。

【００７３】

ホームサーバ１は、動画像データの選択要求についても操作端末の認証を行って、認証に成功した場合についてのみ、その動画像データをテレビ５１に送出し、表示させるように構成される。

【００７４】

〈宅外からのアクセス〉

前述した例では操作端末を宅内で使用される統合型リモコンとしているが、これに代えて宅外からホームサーバ１にアクセスして各機器の操作に関する指示を行うように構成することが考えられる。たとえば、各機器が設置されている住宅外のパソコンや電話機などを利用してインターネット網や電話回線網などを通じて操作の指示を行う場合が考えられる。また、携帯電話やＰＨＳ、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔｓ）などの携帯端末から無線電話網を介して機器操作の指示を行う場合が考えられる。これら操作端末は前述のリモコン３とほぼ同様の構成であり、通信装置４１がそれぞれの通信手段に対応するインターフェイスで構成される。このような場合も、前述と同様にして、パソコン、電話機、携帯電話、ＰＨＳ、ＰＤＡなどの端末ＩＤを予めホームサーバ１に登録しておき、同時に各操作端末の認証処理に用いるための公開鍵をホームサーバ１に登録しておく。電話機や携帯電話、ＰＨＳなどの場合には、端末ＩＤとしてその電話番号を登録するように構成することも可能である。このような操作端末を用いて宅外からアクセスして各機器の操作を行う場合を説明する。ここで、エアコン５５の設定温度を調節する場合を例として説明する。

【００７５】

まず、操作端末から宅内ネットワーク５を介してホームサーバ１にアクセスし、操作端末の端末ＩＤを送信するとともにエアコン５５の現在の状態に関する情報を要求する要求信号を送信する。ホームサーバ１は、図６に示すような操作端末の認証処理を実行し、認証に成功した場合には、宅内ネットワーク５を介してエアコン５５の現在の状態に関する情報を取得し、この情報を操作端末に送信す

る。

【００７６】

ユーザは、操作端末の表示装置４０に表示されるエアコン５５の現在の状態に関する情報を参照し、エアコン５５の電源投入、運転モード変更、設定温度変更などの必要な指示情報を入力する。操作端末では、ユーザから入力された指示情報を操作端末の端末ＩＤとともにホームサーバ１に送信する。

【００７７】

ホームサーバ１はこの指示情報を受信すると、端末ＩＤに基づく端末情報に基づいて再度操作端末の認証処理を実行する。ここで認証に成功した場合には、指示情報に基づいて、エアコン５５の操作に関する制御信号を生成して、エアコン５５の制御を実行する。

【００７８】

このように、操作端末からの指示情報を受信する度に認証処理を行うことにより、第３者からの不正なアクセスを防止することができ、住宅内の各機器を安全に操作することが可能となる。また、ユーザが操作端末の端末ＩＤを意識することなく、ホームサーバ１における操作端末の認証処理が行われるため、ユーザがパスワードなどを記憶しておく必要がなく、第３者にパスワードが漏洩して不正に使用されることを防止できる。

【００７９】

操作端末とホームサーバ１との間の通信において、データを暗号化して送受信するように構成することも可能である。この場合、電話回線網やインターネット網、携帯電話網などの通信経路上において第３者に通信をモニタされた場合であっても、その内容を知られることが防止できる。ここでの暗号化方法は、公開鍵暗号を用いることが可能である。

【００８０】

〈個人情報に基づくアクセス制限〉

ホームサーバ１において、操作端末を操作するユーザの個人情報を管理し、この個人情報に基づいてアクセス制限を行うように構成することができる。たとえば、１つのリモコン３につき１個人を対応付けて個人情報を登録し、この個人情

報に基づいてそのリモコン３からの操作に対する制限を設けることが可能となる。

【００８１】

リモコン３を操作するユーザの個人情報をホームサーバ１に登録する際の手順を図８のフローチャートを用いて説明する。

リモコン３からユーザの個人情報の登録要求があった場合、ステップＳ５１において登録要求のあった操作端末の端末情報を呼び出す。ここでは、端末情報データベース１９から該当する端末ＩＤの端末情報を呼び出す。

【００８２】

ステップＳ５２では、登録要求があった操作端末の端末情報が登録済みであるか否を判別する。登録要求があった操作端末の端末情報が端末情報データベース１９に登録されていると判断した場合にはステップＳ５３に移行し、そうでない場合にはエラーメッセージを送信する処理を終了する。

【００８３】

ステップＳ５３では、操作端末から個人名を受信する。ホームサーバ１はリモコン３に対して個人名の入力を促す入力要求を送信し、これに対応してユーザが入力した個人名データをリモコン３から受信する。

【００８４】

ステップＳ５４では、操作端末から個人情報を受信する。ホームサーバ１はリモコン３に対して個人情報の入力を促す入力要求を送信し、これに対してユーザが入力した個人情報のデータをリモコン３から受信する。ここで、ユーザから入力される個人情報として、たとえば、年齢、性別などの基本データの他に、会員制のサービスを利用する場合のそのサービスに対するパスワードなどを登録することができる。また、クレジットによる買い物やオンラインショッピングなどを利用する際に必要となる住所、電話番号、クレジットカード番号などを登録しておくことも可能である。さらに、リモコン３を使用するユーザの認証を行うために、指紋情報、虹彩情報、網膜情報、声紋情報などの生体情報を登録しておくことも可能である。

【００８５】

ステップＳ５５では、受信した個人名が登録済みであるか否かを判断するために、個人情報データベース２０の情報を読み出す。ステップＳ５６では、受信した個人名が登録されているか否かを判断する。受信した個人名が個人情報データベース２０に登録されていると判断した場合にはステップＳ５８に移行し、そうでないと判断した場合にはステップＳ５７に移行する。

【００８６】

ステップＳ５７では、受信した個人情報を新規に登録する。ここでは、受信した個人情報のレコードを個人情報データベース２０内に新たに作成して格納する。ステップＳ５８では、受信した個人情報に基づいて、個人情報データベース２０内の該当するレコードの内容を更新する。

【００８７】

ステップＳ５９では、操作端末に対応する個人名を記録する。登録要求があったリモコン３と登録された個人情報を関連付けるために、端末情報データベース１９の該当する端末情報に個人名を関連付けて登録する。

【００８８】

このように操作端末を操作するユーザの個人情報を関連付けて登録しておくことによって、個人情報に基づくアクセス制限を行うことが可能となる。ホームサーバ１の蓄積情報データベース２３内に蓄積された情報へのアクセス、ＣＡＴＶや衛生放送の利用について、個人に対するアクセス制限を設定している場合には、操作端末からアクセス要求があった場合に、操作端末の認証を行った後、その操作端末に関連付けられた個人情報を読み出して、操作しているユーザのアクセス権を判定し、アクセスを許可するか否かを決定することができる。

【００８９】

たとえば、操作端末から蓄積情報データベース２０内の情報へのアクセス要求があった場合、ホームサーバ１は要求のあった操作端末の認証処理を実行し、操作端末の認証に成功した場合に、その操作端末に関連付けられた個人情報を個人情報データベース２０から取り出し、要求された情報へのアクセス権を判定してアクセスを許可するか否かを決定する。このことにより、未成年に好ましくないとされる映画や画像データなどが蓄積情報データベース２３に蓄積されているよ

うな場合に、操作端末からのその情報へのアクセス要求があると、ホームサーバ１は端末情報データベース１９からその操作端末に対応する個人名を特定し、この個人名から個人情報データベース２０内の個人情報を取得して、その情報へのアクセス権を判定する。アクセス要求のあった情報が１８歳以上の者にのみアクセス許可するように設定されており、アクセス要求があった操作端末に対応するユーザの個人情報が１８歳未満である場合には、情報へのアクセス要求を拒否する。このような蓄積情報データベース２３に蓄積されている情報のアクセス要求は、テレビ５１への表示を要求する場合が考えられるが、アクセス要求を拒否する場合には、この情報へのアクセス権がない旨のメッセージをテレビ５１の画面またはスピーカーに出力してユーザに知らせるように構成できる。

【００９０】

個人情報の登録および変更については、各操作端末にマスタパスワードを設定しておき、正当なマスタパスワードが入力されたときのみ、実行することが可能であるような構成とすることができる。このことにより、第３者が不正使用を目的として個人情報を改竄することを防止することができる。

【００９１】

〈宅外へのデータ送出〉

宅外において買い物を行う場合には、個人情報データベース２０にクレジットカード番号を予め記憶させておき、登録された操作端末を用いてホームサーバ１を介してクレジット会社と通信を行い、支払の手続きを行うことが考えられる。この場合、ホームサーバ１が宅外ネットワーク７を介してクレジット会社とのデータ通信を行い、クレジットカード番号などの必要事項を送信するため、買い物をした店にクレジットカード番号を知られることがなく、安全に決済を行うことが可能となる。

【００９２】

ＣＡＴＶ、衛星放送などの双方向通信やパソコン５３からインターネットを通じてのオンラインショッピングを行う場合にも、住所、電話番号、クレジットカード番号などを個人情報として登録しておくことにより、この登録情報を用いて簡単にデータ送信を行うことが可能となり、ユーザの手間を省くことが可能とな

る。このような個人情報は、登録されていない操作端末を用いて見ることができないため、第３者に情報が漏洩することを防止できる。

【００９３】

また、会員制の有料コンテンツに宅外からアクセスする場合に、個人情報データベース２０にその有料コンテンツにアクセスするためのパスワードを予め登録しておき、ホームサーバ１によりその有料コンテンツの提供者との通信を行い、有料コンテンツを利用するように構成できる。この場合、ユーザが、各有料コンテンツの提供者毎のパスワードやサービス毎に設定されているパスワードをすべて記憶しておく必要がなく、パスワードが第３者に漏洩することも防止できる。

【００９４】

〈端末情報および個人情報によるアクセス制限〉

端末情報によるアクセス制限と操作端末に関連付けられたユーザの個人情報によるアクセス制限とを統合して、ホームサーバ１に対するアクセス制限を行う場合について、図９のフローチャートに基づいて説明する。ここでも、蓄積情報データベース２３に蓄積されている情報へのアクセス要求があった場合について説明する。

【００９５】

操作端末から蓄積情報データベース２３に蓄積されている情報へのアクセス要求があった場合には、ステップＳ６１において要求された情報の種類についてのデータを蓄積情報データベース２３から取得する。ステップＳ６２では、要求された情報に対してアクセス制限が設定されているか否かを判別する。蓄積情報データベース２３に蓄積された情報には、その情報毎にアクセス制限が設定されている場合と、分類された種類毎にアクセス制限が設定されている場合が考えられる。いずれの場合であっても、アクセス要求があった情報に対してアクセス制限が設定されていないと判断した場合にはステップＳ６３に移行し、アクセス制限が設定されている場合にはステップＳ６４に移行する。

【００９６】

ステップＳ６３では、宅内からのアクセスであるか否かを判別する。アクセス要求を送信してきた操作端末の端末ＩＤから端末情報を取得し、宅内に存在する

操作端末であるか否かを判断し、宅内からのアクセスではないと判断した場合にはこの操作端末からのアクセスを拒否し、蓄積情報データベース２３内に蓄積された該当する情報の提供を行わない。また、宅内からのアクセスであると判断した場合には、この操作端末からのアクセスを許可し、蓄積情報データベース２３内の該当する情報の提供を行う。この場合、アクセス制限が設定されていない情報を宅外からアクセスすることを拒否するように設定しているが、宅外からのアクセスを許可するように構成することも可能である。

【００９７】

ステップＳ６４では、操作端末の認証を行う。前述したように、認証用データ列を送信し、操作端末において秘密鍵で暗号化されたデータ列を受信し、公開鍵を用いて復号化して元の認証用データ列と照合することにより、登録されている正当な操作端末であるか否かの判断を行う。操作端末の認証に失敗した場合には、アクセスを拒否する旨のメッセージを操作端末に送信しこの処理を終了する。操作端末の認証に成功した場合には、ステップＳ６６に移行する。

【００９８】

ステップＳ６６では、個人情報に基づくアクセス制限が設定されているか否かを判別する。アクセス要求があった情報に個人情報によるアクセス制限が設定されていない場合には、操作端末からのアクセス要求を許可する。また、アクセス要求があった情報に個人情報によるアクセス制限が設定されている場合には、ステップＳ６７に移行する。

【００９９】

ステップＳ６７では、アクセス要求を送信してきた操作端末の端末ＩＤに基づいて端末情報データベース１９から対応する端末情報を取得し、これから関連付けられているユーザの個人名を特定し、個人情報データベース２０から該当するユーザの個人情報を取得する。

【０１００】

ステップＳ６８では、取得した個人情報が情報へのアクセス制限を満たしているか否かを判別する。アクセス要求を送信してきた操作端末に関連付けられたユーザの個人情報が、アクセス要求があった情報に設定されているアクセス制限を

満たしていないと判断した場合には、操作端末に対してアクセスを拒否する旨のメッセージを送信しこの処理を終了する。また、アクセス要求を送信してきた操作端末に関連付けられたユーザの個人情報が、アクセス要求があった情報に設定されているアクセス制限を満たしていると判断した場合には、操作端末に対してこの情報の提供を行う。

【０１０１】

このように、アクセス要求を行った操作端末が宅内にあるものか否かの情報、操作端末の端末情報や操作端末に関連付けられたユーザの個人情報などに基づいてアクセス制限を行うことによって、ユーザによる認証処理の手間を軽減し、利便性を保ったままで、第３者による不正なアクセスを防止して、家庭内の情報を保護することが可能となる。

【０１０２】

操作端末を紛失した場合であっても、ホームサーバ１の端末情報データベース１９からその操作端末の情報を末梢することにより、個人情報の記録を削除することなくその操作端末を用いて第３者が不正にアクセスすることを防止できる。

【０１０３】

〈他の実施形態〉

操作端末として携帯電話やＰＨＳなどを用いる場合には、宅内、宅外ともに同一の操作端末で指示情報を送信することが可能となる。この場合、携帯電話やＰＨＳなどのサービス提供会社により提供されている位置情報提供サービスを利用して、操作端末の位置を取得し、これにより宅内であるか宅外であるかの判定を行うように構成することも可能である。

（付記１）

有線または無線の宅内ネットワークを介して住宅内の１以上の機器に接続される機器制御サーバと、前記機器の操作に関する指示信号を有線または無線で送信可能な操作端末とを備える機器制御システムのアクセス制限方法であって、

前記操作端末に設定される固有の識別子を前記操作端末のアクセス権と関連付けるための端末情報の登録を受け付ける段階と、

前記操作端末の識別子と前記機器の操作に関する指示信号とを含む指示情報を受け付ける段階と、

前記指示情報に含まれる前記操作端末の識別子から前記操作端末のアクセス権を判定する段階と、

前記操作端末のアクセス権と前記機器に関する指示信号とに基づいて前記機器の制御を行う段階と、

を含む機器制御システムのアクセス制御方法。

【０１０４】

（付記２）

前記端末情報の登録を受け付ける際に前記操作端末に設定される公開鍵を受け付け、

前記操作端末において秘密鍵で暗号化された所定のデータを受信し、前記公開鍵により復号化して前記所定のデータと照合することによって前記操作端末の認証を行う段階をさらに含む付記１に記載の機器制御システムのアクセス制御方法。

【０１０５】

（付記３）

前記公開鍵は、前記端末情報の一部として前記操作端末の識別子と関連付けられて登録される、付記２に記載の機器制御システムのアクセス制御方法。

【０１０６】

（付記４）

電子情報を取得するとともに蓄積手段内に蓄積する段階をさらに含み、

前記機器に関する指示信号が前記蓄積手段に蓄積された電子情報へのアクセスを含む場合に、前記操作端末のアクセス権に基づいて前記電子情報の提供を許可するか否かを判断する、付記１～３のいずれかに記載の機器制御システムのアクセス制御方法。

【０１０７】

（付記５）

前記機器の操作に関する指示信号が宅外ネットワークへのアクセスを含む場合

に、前記操作端末のアクセス権に基づいて前記宅外ネットワークへのアクセスを許可するか否かを判断し前記機器の制御を行う、付記１～４のいずれかに記載の機器制御システムのアクセス制御方法。

【０１０８】

（付記６）

前記宅外ネットワーク上のコンテンツ毎にアクセスを許可するか否かを判断する、付記５に記載の機器制御システムのアクセス制御方法。

【０１０９】

（付記７）

前記操作端末からの指示情報を受信した際に、前記操作端末が宅内にあるか宅外にあるかを判別し、この判別結果と前記指示情報に含まれる前記操作端末の識別子から前記操作端末のアクセス権を判定する、付記１～６のいずれかに記載の機器制御システムのアクセス制御方法。

【０１１０】

（付記８）

前記操作端末を操作するユーザに関する情報を前記操作端末と関連付けるための個人情報の登録を受け付ける段階をさらに含み、前記指示情報に含まれる前記操作端末の識別子からこの操作端末に関連付けられた個人情報を抽出し、前記個人情報および前記端末情報からアクセス権を判定する、付記１～７のいずれかに記載の機器制御システムのアクセス制御方法。

【０１１１】

（付記９）

付記１～８のいずれかに記載の機器制御システムのアクセス制御方法をコンピュータに実行させるためのプログラム。

【０１１２】

（付記１０）

付記９に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

（付記１１）

有線または無線の宅内ネットワークを介して住宅内の１以上の機器に接続され

、操作端末から送信される前記機器の操作に関する指示信号に基づいて前記機器の制御を行う機器制御サーバであって、

前記操作端末に設定される固有の識別子を前記操作端末のアクセス権と関連付けるための端末情報の登録を受け付ける端末情報受付手段と、

前記端末情報を記憶する端末情報記憶手段と、

前記操作端末の識別子と前記機器の操作に関する指示信号とを含む指示情報を受け付ける指示情報受付手段と、

前記指示情報に基づいて前記操作端末のアクセス権を判定するアクセス権判別手段と、

前記アクセス権判別手段により判定された前記操作端末のアクセス権と前記指示情報に含まれる前記機器の操作に関する指示信号とに基づいて前記機器の制御を行う機器制御手段と、

を含む機器制御サーバ。

【０１１３】

（付記１２）

前記端末情報の登録を受け付ける際に、前記操作端末に設定される公開鍵を受け付け、前記端末情報とともに前記端末情報記憶手段に格納する公開鍵受付手段と、

所定のデータを送信し、前記操作端末において秘密鍵で暗号化された前記所定のデータを受信し、前記公開鍵により復号化して前記所定のデータと照合することによって、前記操作端末の認証を行う操作端末認証手段と、

をさらに含む付記１１に記載の機器制御サーバ。

【０１１４】

（付記１３）

電子情報を取得する電子情報取得手段と、

前記電子情報取得手段により取得した電子情報を蓄積する電子情報蓄積手段とをさらに備え、前記機器に関する指示信号が電子情報蓄積手段に蓄積された電子情報へのアクセスを含む場合に、前記アクセス権判定手段は、前記操作端末のアクセス権を判定して前記電子情報の提供を許可するか否かを判断する、付記１１

または１２に記載の機器制御サーバ。

【０１１５】

（付記１４）

住宅外に存在する宅外ネットワークに接続可能な宅外通信手段をさらに備え、

前記機器の操作に関する指示信号が前記宅外ネットワークへのアクセスを含む場合に、前記アクセス権判定手段は、前記操作端末のアクセス権を判定し前記宅外ネットワークへのアクセスを許可するか否かを判断する、付記１１～１３のいずれかに記載の機器制御サーバ。

【０１１６】

（付記１５）

前記宅外ネットワーク上のコンテンツ毎にアクセスを許可するか否かを判断する、付記１４に記載の機器制御サーバ。

【０１１７】

（付記１６）

前記指示情報受付手段により受け付けた指示情報に基づいて、前記操作端末が宅内にあるか宅外にあるかを判別する端末位置判別手段をさらに備え、前記アクセス権判定手段は、前記端末位置判別手段による判別結果に基づいて前記操作端末のアクセス権を判定する、付記１１～１５のいずれかに記載の機器制御サーバ。

【０１１８】

（付記１７）

前記操作端末を操作するユーザに関する情報を前記操作端末と関連付けるための個人情報の登録を受け付ける個人情報受付手段をさらに含み、前記アクセス権判定手段は、前記指示情報に含まれる前記操作端末の識別子からこの操作端末に関連付けられた個人情報を抽出し、前記個人情報および前記端末情報からアクセス権を判定する、付記１１～１６のいずれかに記載の機器制御サーバ。

【０１１９】

（付記１８）

住宅内の１以上の機器と有線または無線の宅内ネットワークを介して接続され

る機器制御サーバを有する機器制御システムにおける前記機器の操作に関する指示信号を送信する操作端末であって、

固有の識別子を記憶する識別子記憶手段と、

前記機器制御サーバに前記識別子の登録を行う端末情報登録手段と、

前記機器の操作に関する指示入力を受け付ける入力受付手段と、

前記入力受付手段により受け付けた指示入力と、前記識別子記憶手段に記憶されている識別子とに基づいて指示情報を生成する指示情報生成手段と、

前記指示情報生成手段により生成された指示情報を無線または有線により送信する指示情報送信手段と、

を備える操作端末。

【０１２０】

（付記１９）

現在の位置情報を取得する位置情報取得手段をさらに備え、

前記指示情報生成手段は、前記指示入力、前記識別子および前記位置情報取得手段により取得した位置情報に基づいて指示情報を生成する付記１８に記載の操作端末。

【０１２１】

（付記２０）

操作するユーザに関する情報の入力を受け付ける個人情報入力手段をさらに備え、

前記指示情報生成手段は、前記指示入力、前記識別子および前記個人情報入力手段により受け付けたユーザに関する情報に基づいて指示情報を生成する付記１８または１９に記載の操作端末。

【０１２２】

（付記２１）

秘密鍵を記憶する秘密鍵記憶手段と、

前記秘密鍵に対応する公開鍵を記憶する公開鍵記憶手段と、

前記秘密鍵によりデータを暗号化する暗号化処理手段と、

をさらに含み、前記端末情報登録手段により前記機器制御サーバに端末情報の登

録を行う際に前記公開鍵を前記機器制御サーバに送信し、前記指示情報を送信する際に、前記機器制御サーバから受信する所定のデータを前記秘密鍵によって暗号化して認証情報として送信する、付記１８～２０のいずれかに記載の操作端末。

【０１２３】

【発明の効果】

本発明によれば、機器制御サーバへのアクセス権を操作端末毎に設定して操作端末の識別子に関連付けて登録しているため、宅内からアクセスに対しても宅外からのアクセスに対しても、機器の操作に関する指示情報を受け付けることが可能となり、第３者による不正なアクセスを防止するとともに、操作端末毎のパスワードや利用する情報毎のパスワードの設定やこれを記憶する手間を省略することができる。

【図面の簡単な説明】

【図１】

本発明の概略構成を示す説明図。

【図２】

機器制御サーバの概略構成を示すブロック図。

【図３】

操作端末の概略構成を示すブロック図。

【図４】

機器制御サーバにおける登録受付処理を示すフローチャート。

【図５】

操作端末における登録処理を示すフローチャート。

【図６】

機器制御サーバにおける端末認証処理を示すフローチャート。

【図７】

端末認証処理時の操作端末の動作を示すフローチャート。

【図８】

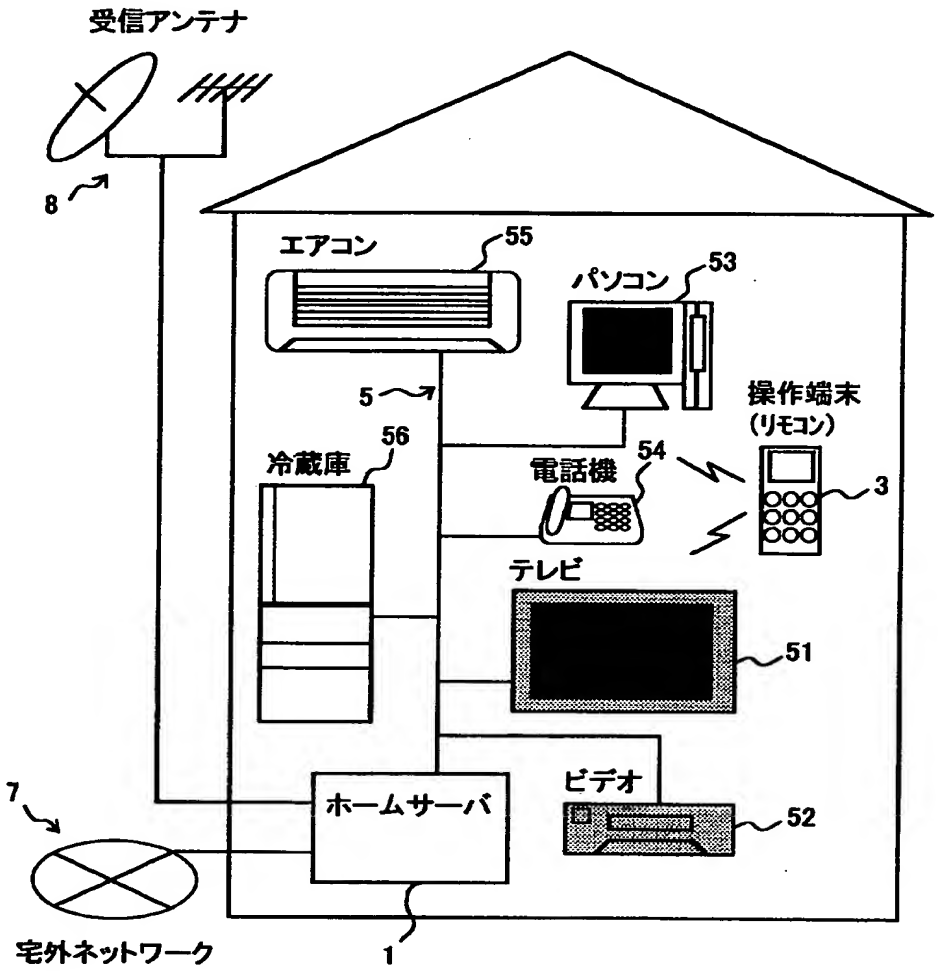
個人情報登録処理を示すフローチャート。

【図９】

端末情報と個人情報とを用いたアクセス制限の処理を示すフローチャート。

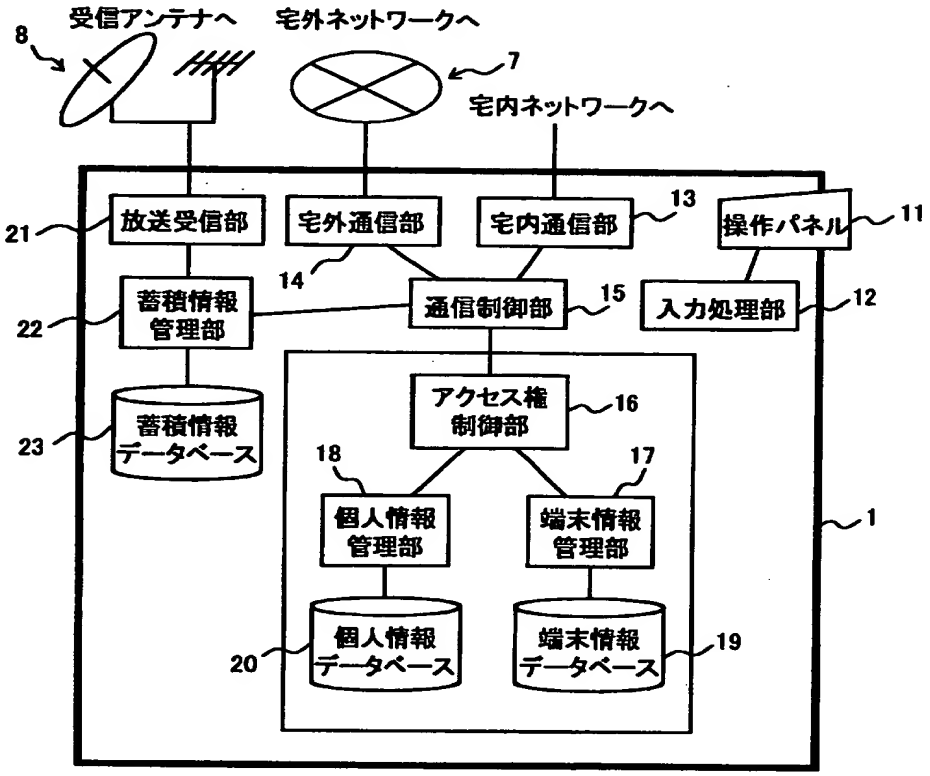
【書類名】　　図面

【図１】

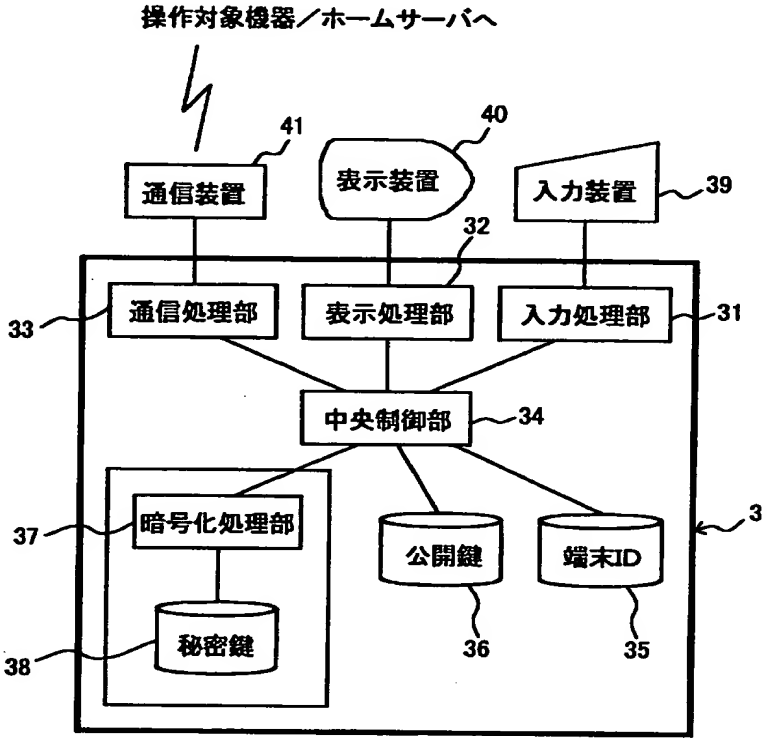


出証特２００１－３０７１３１３

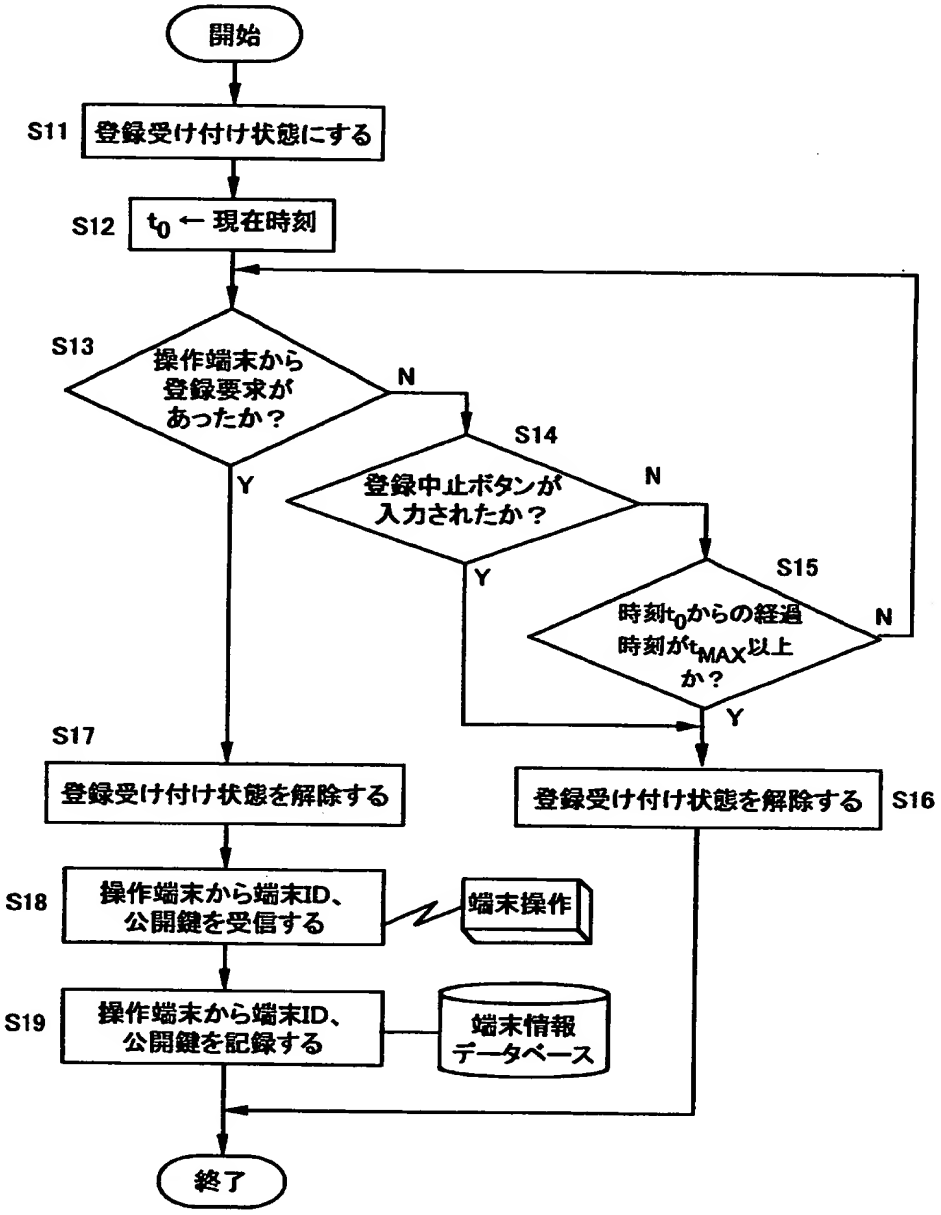
【図２】


受信アンテナへ
宅外ネットワークへ
8
7
宅内ネットワークへ
21
放送受信部
宅外通信部
宅内通信部
13
操作パネル
11
14
蓄積情報
管理部
22
通信制御部
15
入力処理部
12
アクセス権
制御部
16
蓄積情報
データベース
23
18
17
個人情報
管理部
端末情報
管理部
1
個人情報
データベース
20
端末情報
データベース
19

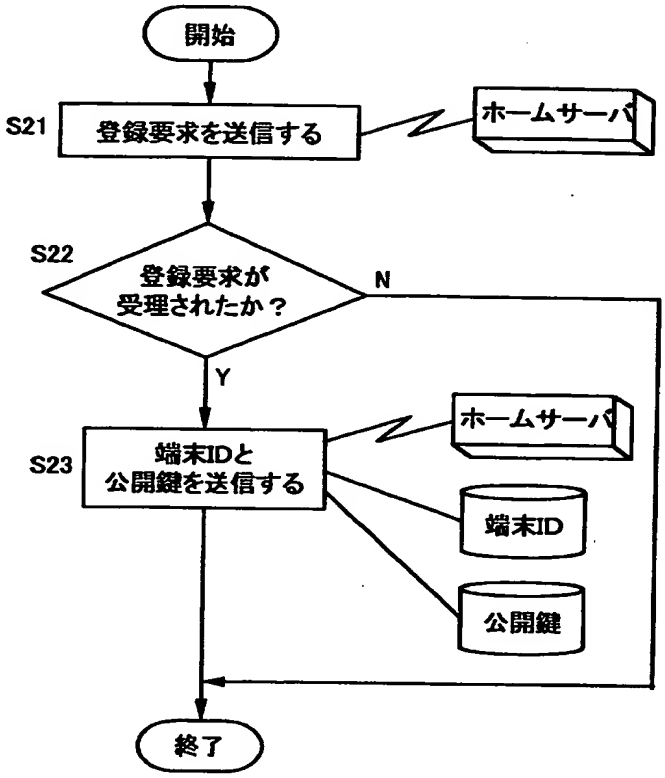
【図３】


操作対象機器／ホームサーバへ
41
40
通信装置
表示装置
入力装置
39
32
通信処理部
表示処理部
入力処理部
33
31
中央制御部
34
暗号化処理部
37
公開鍵
端末ID
3
秘密鍵
38
36
35

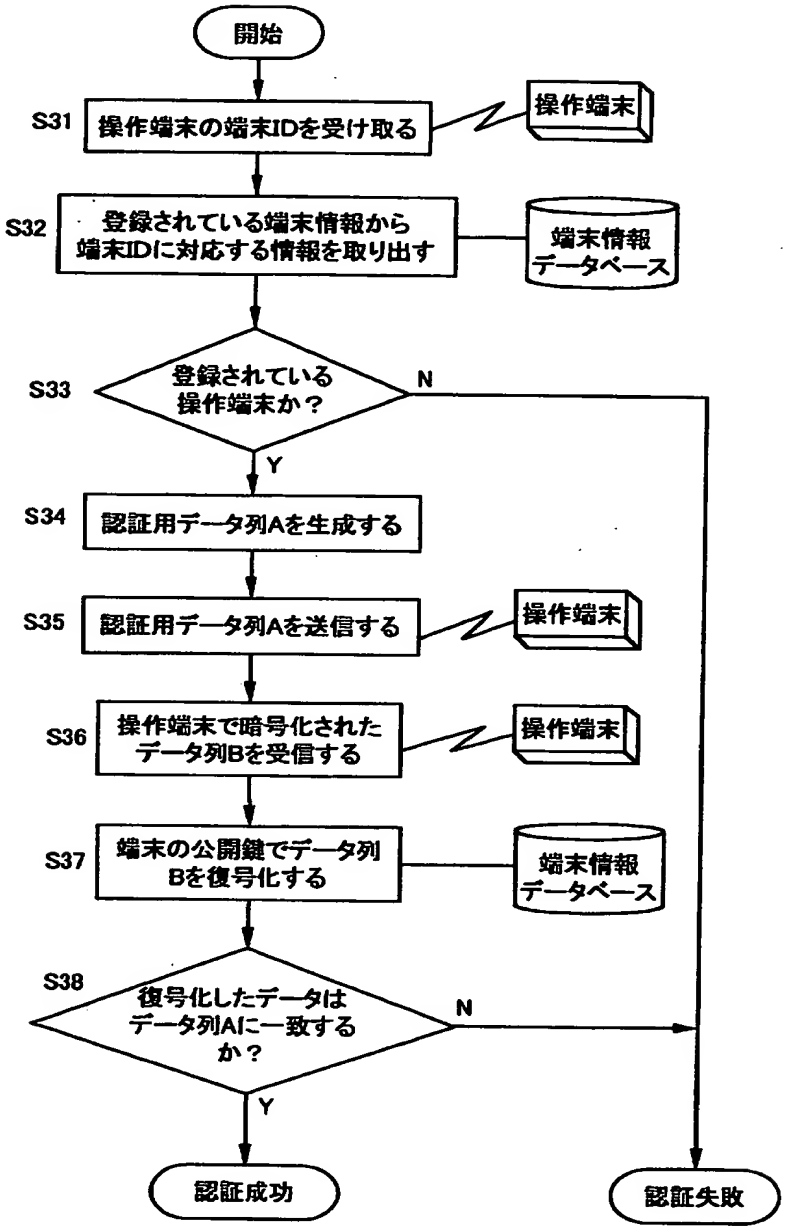
【図４】


開始
S11
登録受け付け状態にする
S12
t_0 ← 現在時刻
S13
操作端末から登録要求があったか？
N
Y
S14
登録中止ボタンが入力されたか？
N
Y
S15
時刻t_0からの経過時刻がt_{MAX}以上か？
N
Y
S17
登録受け付け状態を解除する
S16
登録受け付け状態を解除する
S18
操作端末から端末ID、公開鍵を受信する
端末操作
S19
操作端末から端末ID、公開鍵を記録する
端末情報データベース
終了

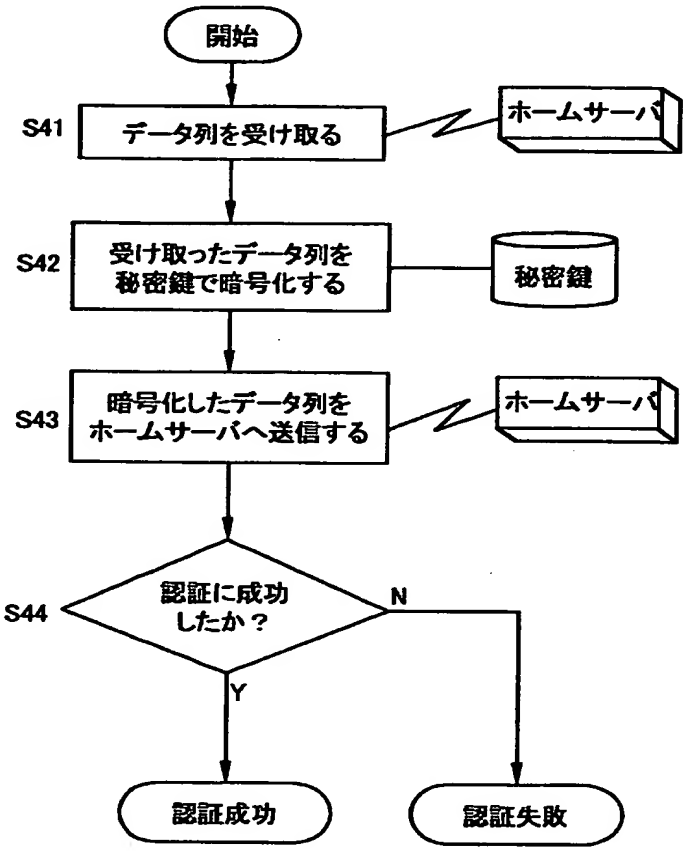
【図５】


開始
S21
登録要求を送信する
ホームサーバ
S22
登録要求が
受理されたか？
N
Y
S23
端末IDと
公開鍵を送信する
ホームサーバ
端末ID
公開鍵
終了

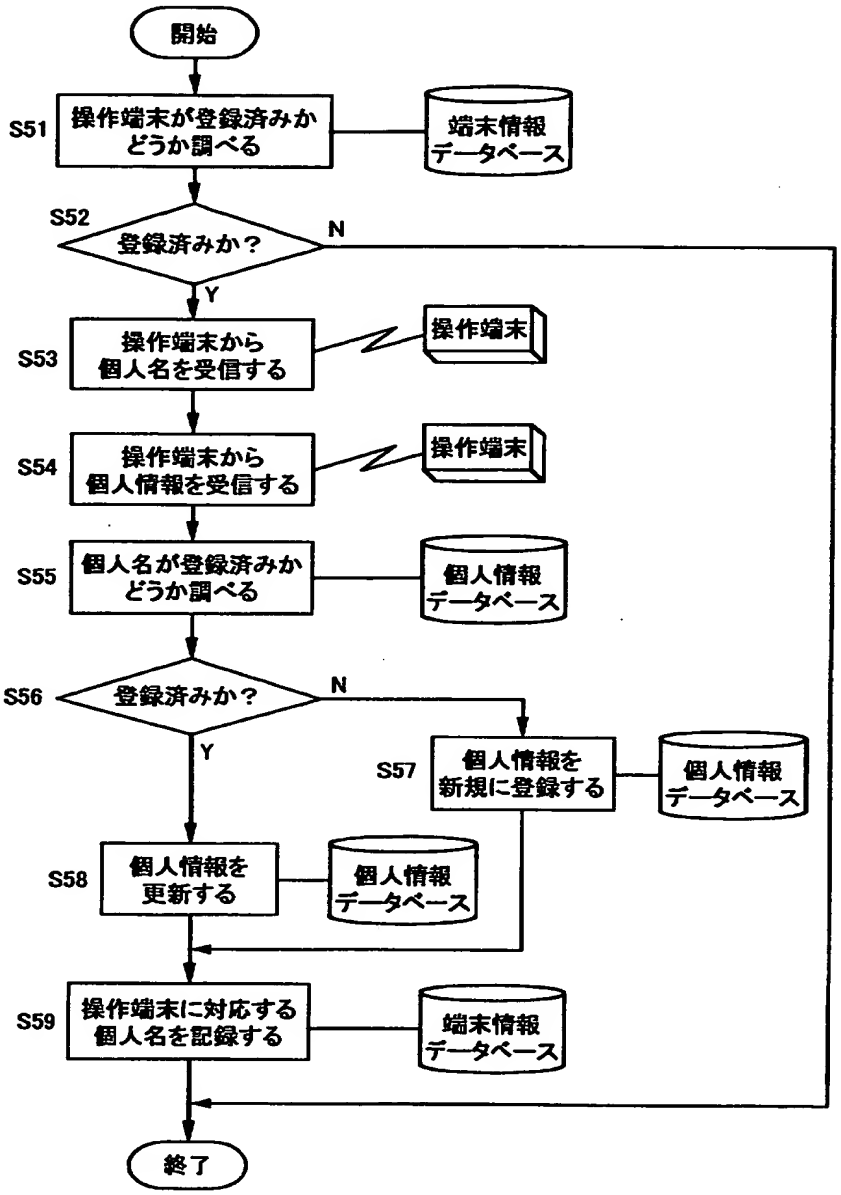
【図６】


開始
S31
操作端末の端末IDを受け取る
操作端末
S32
登録されている端末情報から
端末IDに対応する情報を取り出す
端末情報
データベース
S33
登録されている
操作端末か？
N
Y
S34
認証用データ列Aを生成する
S35
認証用データ列Aを送信する
操作端末
S36
操作端末で暗号化された
データ列Bを受信する
操作端末
S37
端末の公開鍵でデータ列
Bを復号化する
端末情報
データベース
S38
復号化したデータは
データ列Aに一致する
か？
N
Y
認証成功
認証失敗

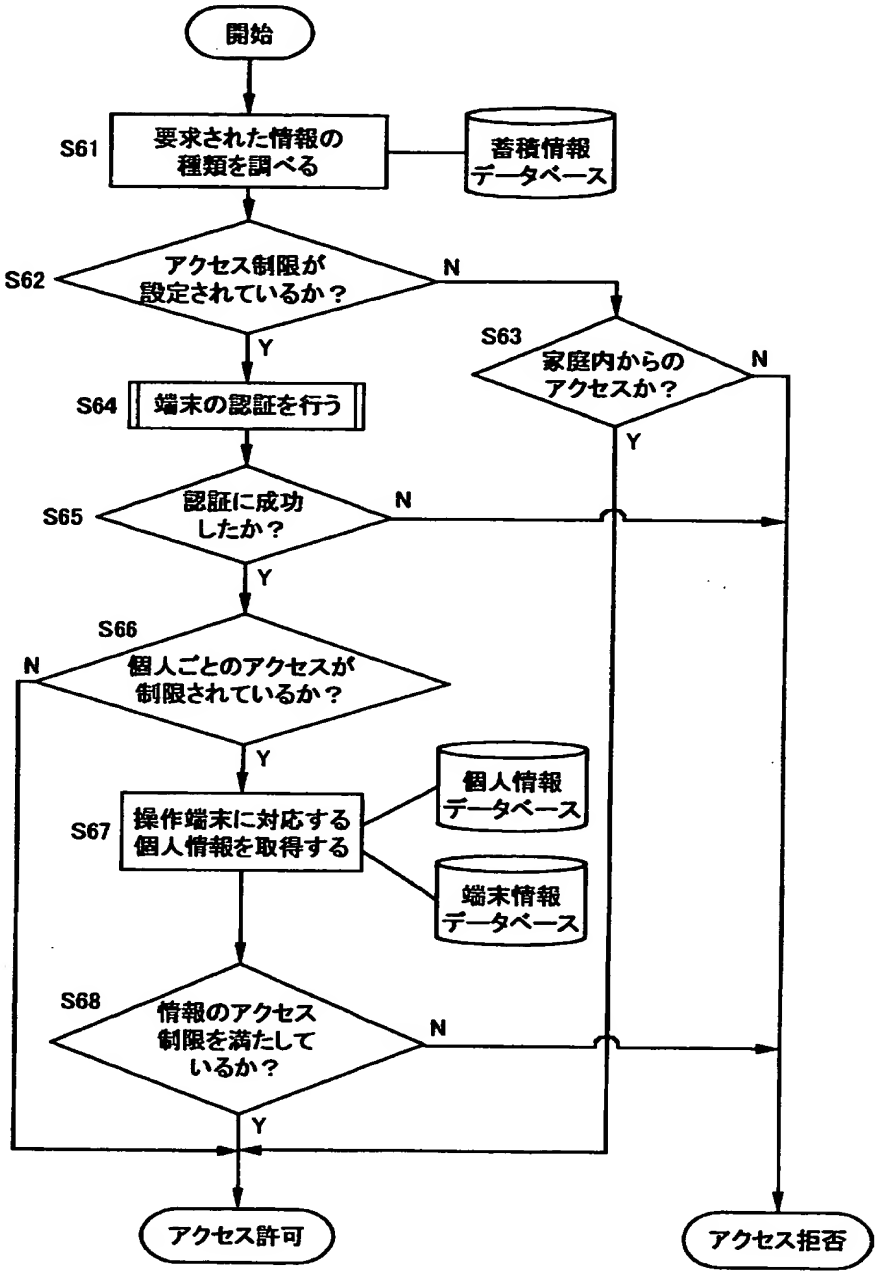
【図７】


開始
S41
データ列を受け取る
ホームサーバ
S42
受け取ったデータ列を
秘密鍵で暗号化する
秘密鍵
S43
暗号化したデータ列を
ホームサーバへ送信する
ホームサーバ
S44
認証に成功
したか？
N
Y
認証成功
認証失敗

【図８】


開始
S51
操作端末が登録済みか
どうか調べる
端末情報
データベース
S52
登録済みか？
N
Y
S53
操作端末から
個人名を受信する
操作端末
S54
操作端末から
個人情報を受信する
操作端末
S55
個人名が登録済みか
どうか調べる
個人情報
データベース
S56
登録済みか？
N
Y
S57
個人情報を
新規に登録する
個人情報
データベース
S58
個人情報を
更新する
個人情報
データベース
S59
操作端末に対応する
個人名を記録する
端末情報
データベース
終了

【図９】


開始
S61
要求された情報の種類を調べる
蓄積情報データベース
S62
アクセス制限が設定されているか？
N
Y
S63
家庭内からのアクセスか？
N
Y
S64
端末の認証を行う
S65
認証に成功したか？
N
Y
S66
個人ごとのアクセスが制限されているか？
N
Y
S67
操作端末に対応する個人情報を取得する
個人情報データベース
端末情報データベース
S68
情報のアクセス制限を満たしているか？
N
Y
アクセス許可
アクセス拒否

【書類名】　　要約書

【要約】

【課題】　住宅内の機器を制御する機器制御システムにおいて、利用者の認証作業の手間を軽減するとともに、第３者からの不正なアクセスを防止する。

【解決手段】　操作端末に設定される固有の識別子を操作端末のアクセス権と関連付けるための端末情報の登録を受け付ける段階と、操作端末の識別子と機器の操作に関する指示信号とを含む指示情報を受け付ける段階と、指示情報に含まれる操作端末の識別子から操作端末のアクセス権を判定する段階と、操作端末のアクセス権と機器に関する指示信号とに基づいて前記機器の制御を行う段階とを含む機器制御システムのアクセス制御方法。

【選択図】　　図２

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社